RSA SecurID Access SAML Configuration for ThoughtWorks Mingle

Last Modified: February 15, 2017

ThoughtWorks Mingle released in May 2007, is a software for agile project management and collaboration. It was released as a SaaS offering in 2013. Mingle's Planner features are useful to define objectives for the organization, track a plan's progress, and receive alerts when a plan changes.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and ThoughtWorks Mingle.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from IDR portal.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	*https://testsso1.mingle.thoughtworks.com/*
ACS URL	*https://profile.thoughtworks.com/saml/consume*
Service Provider Issuer ID	*https://profile.thoughtworks.com/*

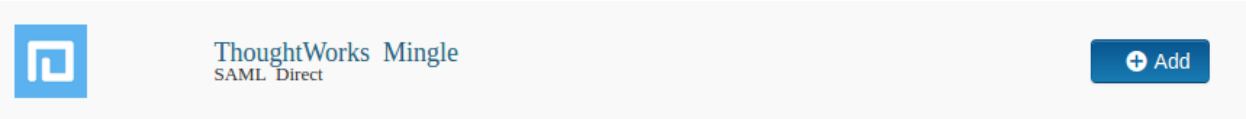
Procedure

1. Add the Application in RSA SecurID Access
2. Configure ThoughtWorks Mingle to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

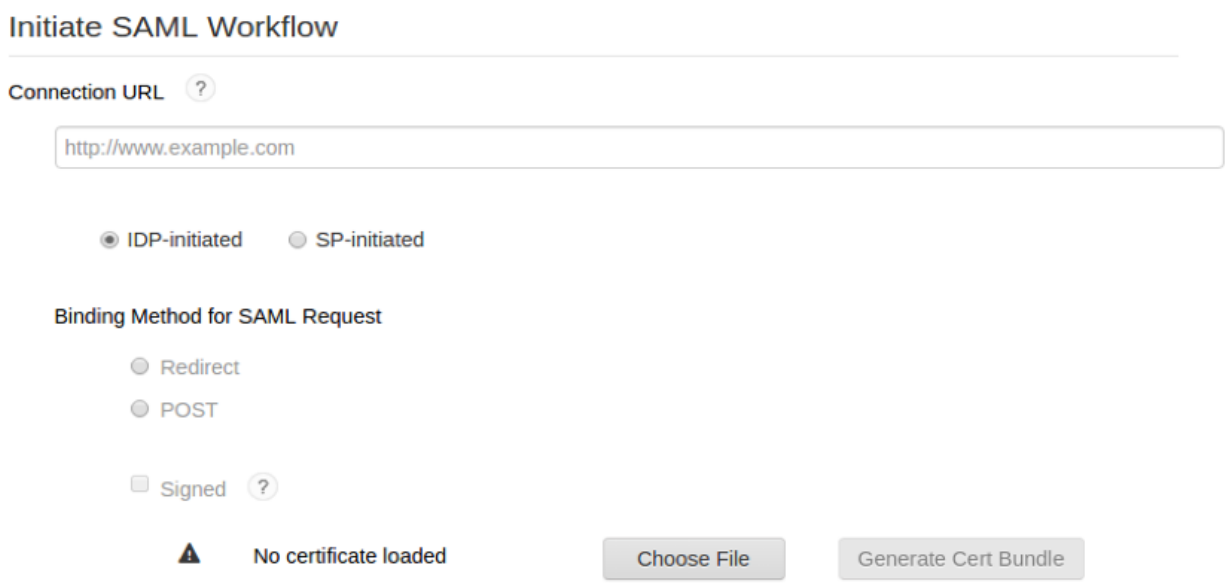
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** ThoughtWorks Mingle.



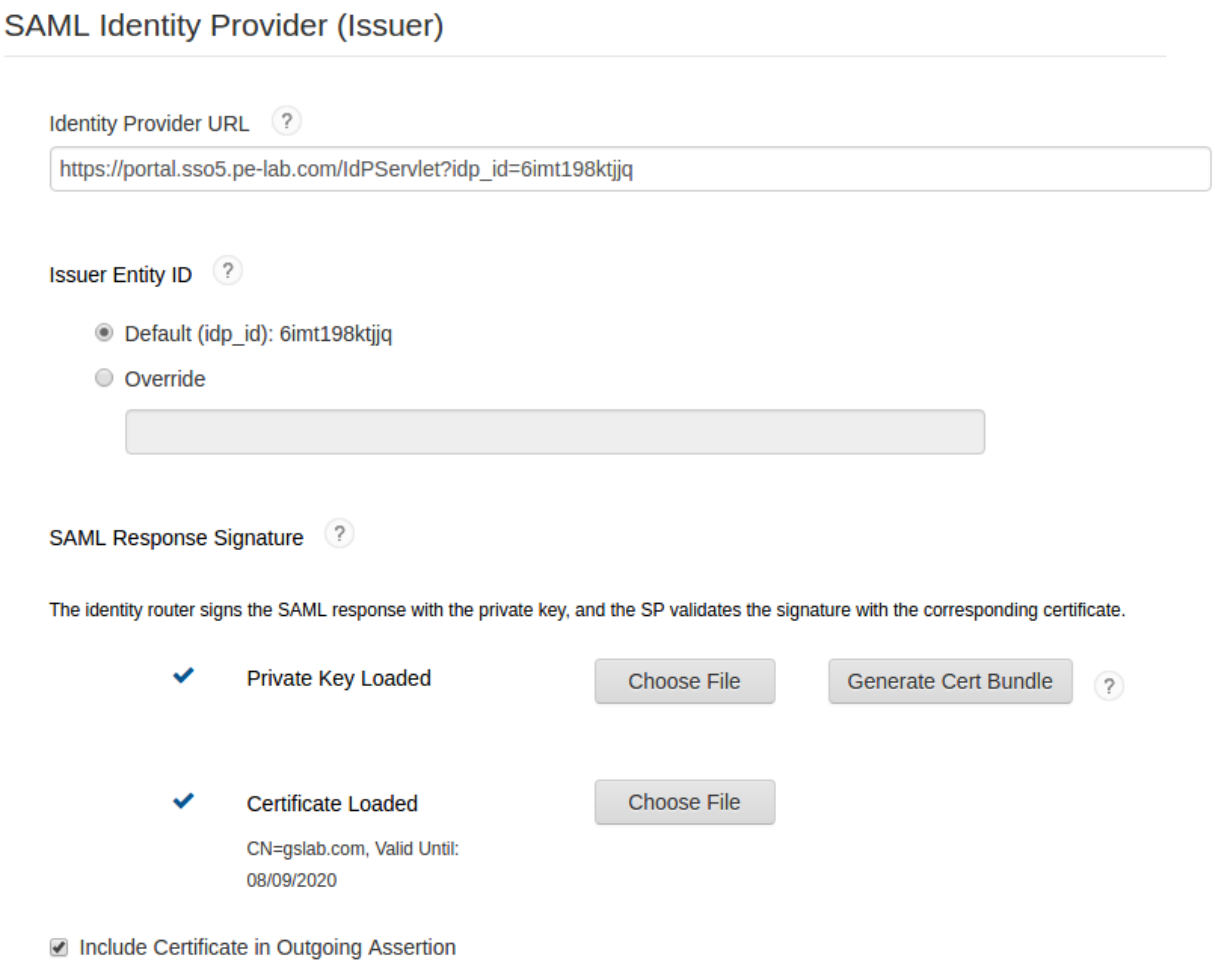
3. On the Basic Information page, specify the application name and click **Next Step**.

4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP–initiated**.

Note: The following IdP-initiated configuration works for SP-initiated ThoughtWorks Mingle connections as well.



5. Scroll down to **SAML Identity Provider (Issuer)** section.

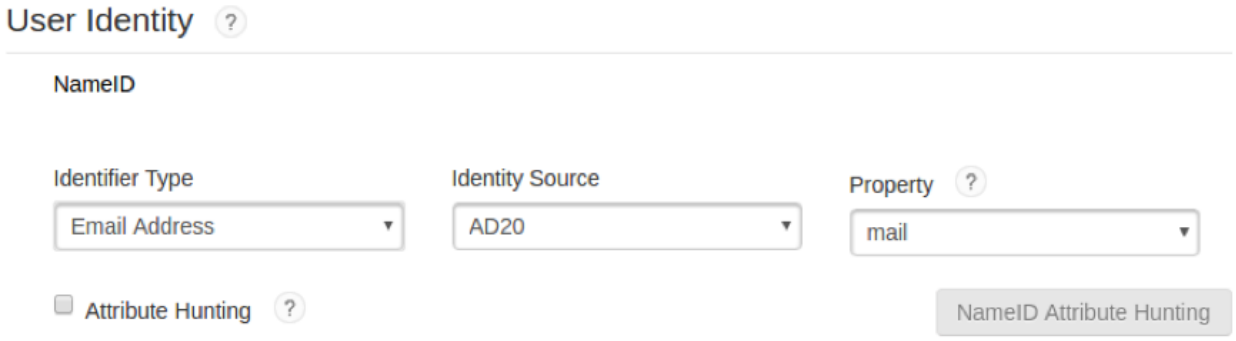


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

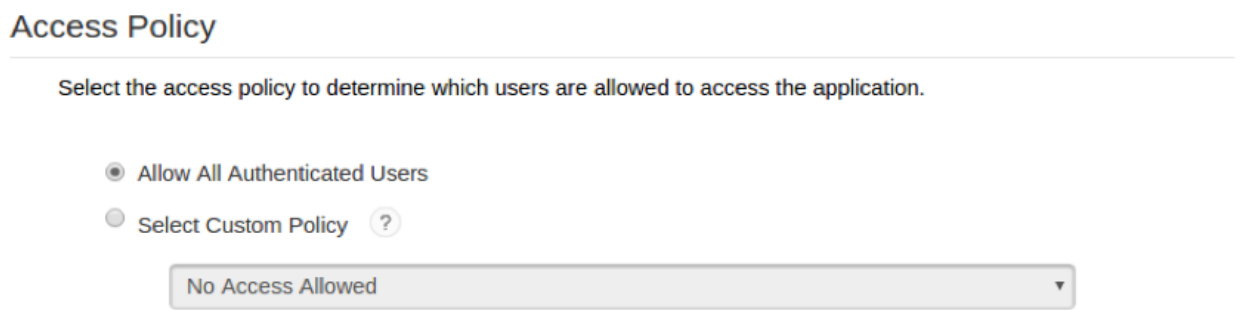
6. Scroll down to the **Service Provider** section.

   a. In the **Assertion Consumer Service (ACS) URL** field, insert value as provided by Service Provider.
   b. In the **Audience (Service Provider Entity ID)** field, insert value as provided by Service Provider.

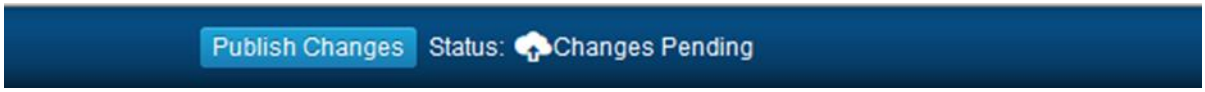
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be in presented in email format and the user account will be validated against the User Store selected.



8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the drop down list.



10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



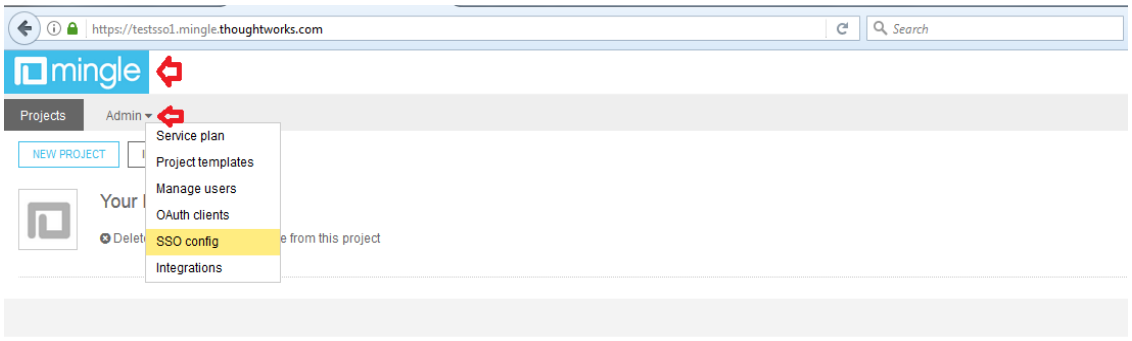
14. Navigate to **Applications > My Applications**.
15. Locate ThoughtWorks Mingle in the list and from the **Edit** pulldown select **Export Metadata**.

Configure ThoughtWorks Mingle to Use RSA SecurID Access as an Identity Provider

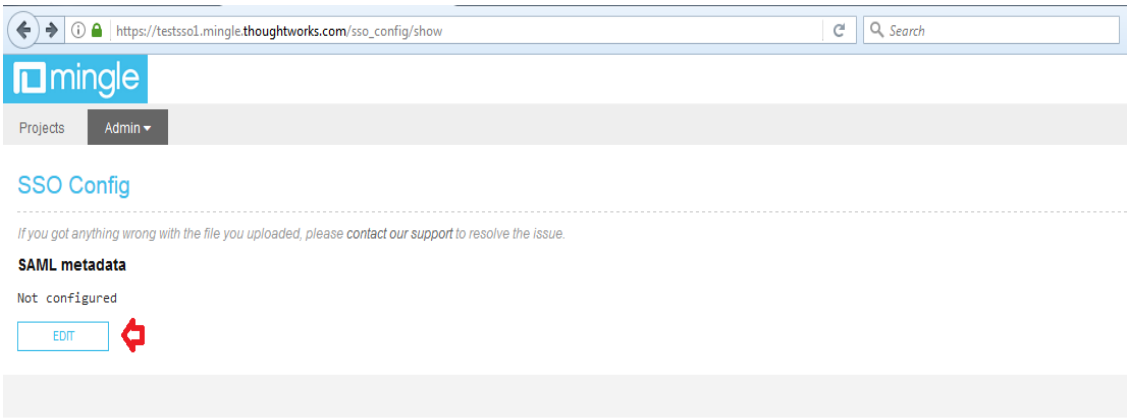
Procedure

1. Login to your ThoughtWorks Mingle account. (https://profile.thoughtworks.com/cas/testsso1/login?url=https://testsso1.mingle.thoughtworks.com/profile/login)

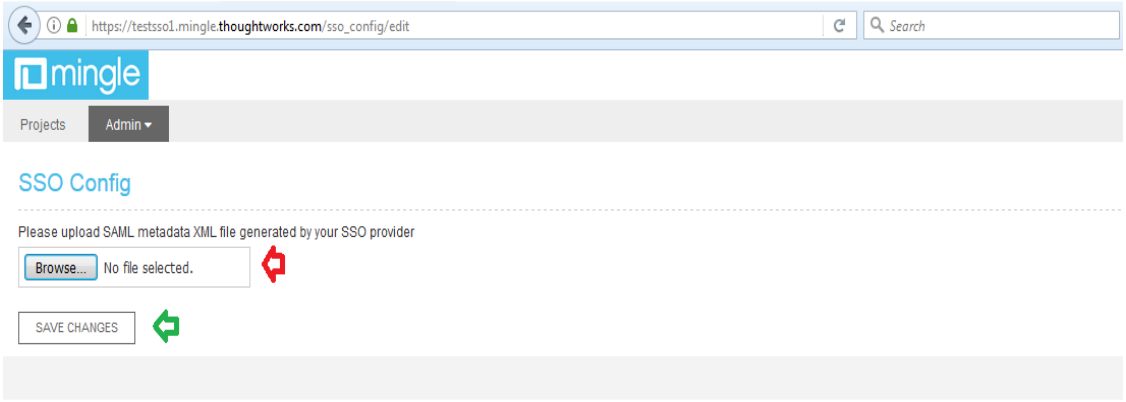
2. Click on **Mingle Logo** followed by **Admin -> SSO config** option to start with SAML configuration.



3. Following UI will be displayed. Click on **EDIT** button to provide SAML configuration details.



4. Following UI will be displayed. ThoughtWorks Mingle allows configuring of SAML via metadata file only as of now. Use IdP metadata file here that you downloaded in Step – 15 above while IdP configuration.



5. Click on **SAVE CHANGES** button to save SAML configurations.

Your ThoughtWorks Mingle account is now enabled for SAML authentication.

RJ